In the Claims:

Please amend the claims as indicated below.

1. (cancelled)

2. (cancelled)

3. (cancelled)

4. (cancelled)

5. (cancelled)

6. (previously presented) A method of providing security against unauthorized access to internal resources of a network device comprising:

receiving a digital signature at a security association manager (SAM);

said SAM requesting a de-encryption code;

said SAM de-encrypting said digital signature with said de-encryption code;

said SAM authenticating said de-encrypted digital signature;

said SAM requesting allowed operations associated with said authenticated signature;

a policy server receiving said request for allowed operations associated with said authenticated signature;

said policy server comparing said authenticated signature with information stored on said policy server; and

said policy server sending a response to said SAM indicating an access level corresponding to said authenticated signature.

7. (Original) A method of providing security according to Claim 6 further comprising:

said policy server authenticating said request for allowed operations associated with said authenticated signature prior to comparing said authenticated signature with said information stored on said policy server.

8. (cancelled)

9. (cancelled)

10. (cancelled)

11. (cancelled)

12. (previously presented) Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

a security association manager (SAM) configured to receive a digital signature;

wherein said SAM is configured to send a message including a portion of said digital signature;

wherein said message includes a request for an encryption decoder;

wherein said SAM is further configured to receive a response to said message; and

wherein said SAM is configured to send a digitally signed message requesting an access level for program code associated with said digital signature, in response to receiving said response message;

a policy server configured to receive said request for allowed operations associated with said authenticated signature;

said policy server including a comparison device configured to compare said authenticated signature with information stored on said policy server; and

said policy server being configured to send a response to said SAM indicating an access level corresponding to said authenticated signature.

13. (cancelled)

14. (cancelled)

15. (cancelled)

16. (cancelled)

17. (cancelled)

18. (currently amended) Apparatus for providing security against unauthorized access to internal resources of a network device comprising:

means, within a security association manager, for receiving a digital signature ~~including an encryption code~~;

means, within said security association manager, for accessing a de-encryption code associated with said digital signature, and for decrypting and authenticating said digital signature ~~in electrical communication with said means for receiving~~; and

means, within a policy server, for receiving a request for allowed operations associated with said authenticated digital signature policy server~~for determining allowed operations associated with said digital signature~~; and

means, within said policy server, responsive to said request, and to a comparison of said authenticated digital signature with information within said policy server, for ~~receiving a downloadable filing including said digital signal and assigning~~ determining an access level for ~~to~~ a java thread associated with said digital signature, and for sending an indication of said access level in a response to said security association manager.